CLAIMS

I claim:

1. A method for key management, comprising:

generating a set of encrypted bits at a security server;

transmitting said set of encrypted bits from said security server to an application server;

broadcasting said set of encrypted bits from said application server to a plurality of recipients, said set of encrypted bits comprising information for generating a set of encryption/decryption bits;

transmitting said set of encrypted bits from a first recipient to said security server;

authenticating said first recipient at said security server;

transmitting a first set of bits from said security server to said first recipient if said first recipient is authenticated, said first set of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of encryption bits;

generating said set of encryption bits at said first recipient from said first set of bits;

encrypting a data stream at said first recipient using said set of encryption bits to form a first encrypted data stream; and

broadcasting said first encrypted data stream from said first recipient with said set of encrypted bits to a plurality of receivers.

2. The method of Claim 1, wherein said set of

encrypted bits further comprises information selected from the group consisting of a policy, a message digest, and a date and time stamp.

3. The method of Claim 2, wherein said policy comprises information selected from the group consisting of security levels of said recipients and classification of said data stream.

4. The method of Claim 1, wherein said authenticating comprises:

establishing a private access line ("PAL") between said security server and said first recipient, comprising:

transmitting an identification of said first recipient to said security server;

decrypting said set of encrypted bits at said security server to obtain access information; and

comparing said identification to said access information to establish authentication when said identification matches said access information.

5. The method of Claim 1, further comprising:

transmitting said set of encrypted bits from a first receiver to said security server;

authenticating said first receiver at said security server;

transmitting a second set of bits from said security server to said first receiver if said first receiver is authenticated, said second set

of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of decryption bits;

generating at said first receiver said set of decryption bits from said second set of bits; and

decrypting said first encrypted data stream using said set of decryption bits at said first receiver.

6. The method of Claim 1, wherein said broadcasting said first encrypted data stream further comprises:

dividing said first encrypted data stream into a plurality of data sections; and

attaching said set of encrypted bits to each of said data sections, each said data section having a corresponding offset value, said offset value is an offset between the starting address of said first encrypted data stream and the starting address of said data section.

7. The method of Claim 1, wherein said application server comprises a memory for storing said set of encrypted bits and a corresponding set of bits containing said information for generating a set of encryption/decryption bits.

8. The method of Claim 7, further comprising comparing said set of encrypted bits to a plurality of sets of encrypted bits in said memory.

9. The method of Claim 8, further comprising

returning a set of bits corresponding to a stored set of encrypted bits from said memory if said set of encrypted bits matches said stored set of encrypted bits.

10. The method of Claim 8, wherein said set of encrypted bits fails to match any of said stored set of encrypted bits in said memory, further comprising:

transmitting an identification of said first receiver to said security server;

decrypting said set of encrypted bits at said security server to obtain access information; and

comparing said identification of said receiver to said access information to establish authentication when said identification matches said access information.

11. The method of Claim 10, further comprising storing said set of encrypted bits and said corresponding set of bits containing said information for generating a set of encryption/decryption bits in said memory subsequent to said authentication.

12. The method of Claim 11, further comprising deleting a least recently used set of encrypted bits and its corresponding set of bits from said memory when said memory is full.

13. The method of Claim 1, further comprising broadcasting said first encrypted data stream in datagram packets, wherein said set of encrypted bits is attached to each of said datagram packets.

14. The method of Claim 1, further comprising:

appending said set of encrypted bits to said first encrypted data stream; and

transmitting a second encrypted data stream from said first receiver to said first recipient, wherein a second set of encrypted bits is appended to said second encrypted data stream.

15. A method for synchronizing keys for streaming media, comprising:

dividing an encrypted data stream into a plurality of encrypted data sections;

generating an offset value for each encrypted data sections, said offset value being an offset between the starting address of said encrypted data stream and the starting address of said encrypted data section;

attaching a set of encrypted bits and said offset value to each of said encrypted data sections to form a data stream; and

broadcasting said data stream.

16. A method for opening a seal, wherein said seal comprises a set of encrypted bits comprising information for generating a set of encryption/decryption bits, comprising:

providing a client having a memory for storing previously opened seals and their corresponding permits, each of said permits being a subset of a corresponding seal and containing information for generating said set of

encryption/decryption bits;

transmitting said seal from a security server to said client; and

comparing said seal to said previously opened seals in said memory.

17. The method of Claim 16, further comprising returning a permit corresponding to a first previously opened seal from said memory if said seal matches said first previously opened seal.

18. The method of Claim 16, further comprising:

transmitting said seal and an identification from said client to said security server if said seal fails to match any of said previously opened seals in said memory;

decrypting said seal at said security server to obtain access information; and

comparing said identification with said access information to obtain authentication if said identification matches said access information.

19. The method of Claim 18, further comprising storing said seal and its corresponding permit in said memory if said client is authenticated.

20. The method of Claim 19, further comprising deleting a least recently used previously opened seal and its corresponding permit when said memory is full prior to said storing.

21. A method for key synchronization, comprising transmitting a plurality of datagram packets from a first party to a second party, each datagram packet having a seal attached, said seal being a set of encrypted bits comprising information for generating a set of encryption/decryption bits.

22. A method for key exchange and synchronization over a duplex channel, comprising:

transmitting a first encrypted data stream having a first seal appended to the head of said first encrypted data stream from a first party to a second party, said first seal being a first set of encrypted bits comprising information for generating a first set of encryption/decryption bits; and

transmitting a second encrypted data stream having a second seal appended to the head of said second data stream from said second party to said first party, said second seal being a second set of encrypted bits comprising information for generating a second set of encryption/decryption bits.

23. The method of Claim 22, further comprising:

transmitting said first seal from said second party to a security server;

authenticating said second party at said security server; and

transmitting a first permit from said security server to said second party if said second party is authenticated, said first permit

being a subset of said first seal, in decrypted form, and containing information for encrypting/decrypting said first encrypted data stream.

24. The method of Claim 23, further comprising:

generating a first set of decryption bits at said second party; and

decrypting said first encrypted data stream at said second party using said first set of decryption bits.

25. The method of Claim 24, further comprising:

transmitting said second seal from said first party to said security server;

authenticating said first party at said security server; and

transmitting a second permit from said security server to said first party if said first party is authenticated, said second permit being a subset of said second seal, in decrypted form, and containing information for encrypting/decrypting said second encrypted data stream.

26. The method of Claim 25, further comprising:

generating a second set of decryption bits at said first party; and

decrypting said second encrypted data stream at said first party using said second set of decryption bits.